

Forensics is the use of science and technology to investigate and establish facts of interest to the legal system. Computer forensics deals with the preservation, identification, extraction and documentation of computer evidence. Evidence exists on computers in many places and formats. In addition to evidentiary documents themselves, operating systems and programs leave a vast array of evidentiary artifacts that can be used to establish the guilt or innocence of accused parties. Computer forensics has been described as the autopsy of a computer hard drive because specialized software tools and techniques are required to analyze the various levels at which computer data has been stored after the fact.

Computer forensics, once a discipline restricted to a small group of law enforcement officers, is now a booming business. Demand for services is exploding as electronic evidence becomes widely used in court, and as companies become concerned about the use of computer networks for corporate spying and other mischief.

Gain the knowledge and skills needed for this technology with Heathkit's Computer Forensics course. Heathkit...the industry's leading company.

Computer Forensics

CFS-100



Quick View

- ▶ Students learn the skills and technology used for the preservation, identification, extraction and documentation of forensic evidence from computers
- ▶ Flexible and Modular Curriculum

System Components

- ▶ CF-100 Textbook
- ▶ CF-100-40 Workbook
- ▶ CF-100-30 Parts Pack
- ▶ CF-100-50 Instructor's Guide

Optional Materials

Instructor Support Module (ISM)

- ▶ PowerPoint Presentations (.ppt and .html versions)

Exercises

- ▶ 31

Prerequisites

- ▶ Basic knowledge of computer use and function



Computer Forensics

Course Objectives

After you complete this course, you will be able to:

- ▶ Acquire computer-related evidence without altering or damaging it. Authenticate that it is the same as the originally-seized data.
- ▶ Analyze and interpret computer-related evidence to determine the user's prior computer activities
- ▶ Ensure that "forensically sterile" conditions are established and maintained throughout the investigation.
- ▶ Follow standard police procedures for collecting computer forensic evidence and establish a chain of custody.
- ▶ Demonstrate the proper use of Forensic Toolkit (FTK), FTK Imager, Password Recovery Toolkit (PRTK), registry Viewer and Known File Filter (KFF).
- ▶ Examine metadata and explain the types of information found there.
- ▶ Determine the partition structure of the drive from which the image was taken, including the size and the file system used in each partition.
- ▶ View data hidden in unpartitioned space, file slack space and unallocated clusters.
- ▶ Recover orphan and previously deleted files and folders. Recover files from recently formatted disks.
- ▶ Immediately identify files that can be safely ignored, illicit files, and flag other files that seem suspicious.
- ▶ Decrypt encrypted files.

Course Objectives

(continued)

- ▶ Demonstrate techniques that speed password recovery, including creating biographical dictionaries and importing custom dictionaries.
- ▶ Examine, decode, and recover evidence from the Windows Registry.
- ▶ Recover "remembered" passwords from a suspect's Registry.
- ▶ Prove that a particular file was once on the suspect's drive, even after the file has been deleted and totally overwritten.
- ▶ Identify email clients, their file format and recover emails.
- ▶ Perform both live and indexed searches.
- ▶ Conduct *stemming*, *phonic*, *synonym*, and *fuzzy* searches and explain when each should be used.
- ▶ Construct regular expressions to find a particular data pattern and perform regular expressions searches.
- ▶ Demonstrate automatic and manual data-carving techniques to recover files.
- ▶ Given a case scenario and an image that contains evidence pertinent to that scenario, find and report that evidence.
- ▶ Explain how the recycle bin works and explore the forensic evidence trail that it leaves.
- ▶ Point out the user's Recent folder and the Internet Explorer's temporary cache and explain what you can expect to find there.

Exercises

- ▶ The Challenges of Computer Forensics
- ▶ Installing Forensic Software
- ▶ Forensically Wiping Media
- ▶ Previewing an Image
- ▶ Making a Forensic Image
- ▶ Processing an Image with Forensic Toolkit (FTK)
- ▶ Working with the FTK Interface
- ▶ Exploring Metadata
- ▶ Creating a New Case
- ▶ Customizing the FTK Interface
- ▶ The FTK Case Logs and Containers
- ▶ Using the Hexadecimal Viewer
- ▶ Working with Graphics
- ▶ Working with Thumbnails
- ▶ Working with Email
- ▶ Working with Filters
- ▶ Indexed Search Techniques
- ▶ Live Search Techniques
- ▶ Recovering Passwords
- ▶ Finding Evidence in the Registry
- ▶ Automatic Data Carving
- ▶ Manual Data Carving
- ▶ The Recycle Bin, the Recent Folder and TIF
- ▶ Putting It All Together
- ▶ Solving a Case
- ▶ Restoring the Computer